Лабораторна робота №2 — Windows Event Log для цифрової криміналістики

Мета роботи

- Ознайомитися з архітектурою Windows Event Logging (EVT (Event Log file format, legacy)/EVTX (Event Log file format, XML-based), служба Windows Event Log Service).
- Навчитися орієнтуватися у категоріях журналів та типах подій.
- Навчитися фільтрувати, експортувати й інтерпретувати події для потреб розслідувань інцидентів.

Теоретична частина

1. Архітектура та формати

- Windows Event Log складається з джерел подій, каналів (logs) і записів (events).
- Файли журналів зберігаються у форматі EVTX за шляхами на кшталт:
    - System, Application, Security: C:\Windows\System32\winevt\Logs*.evtx
    - Спеціальні журнали додатків і сервісів: Applications and Services Logs
- Запис події містить: Event ID, Level (Information, Warning, Error, Critical, Success Audit, Failure Audit), TimeCreated, Provider (джерело), Task/Opcode, Keywords, User, Computer, Channel, а також розділ EventData/Details із полями.

2. Основні канали (журнали)

- Windows Logs
    - Application — події користувацьких застосунків і служб.

    - Security — події аудиту безпеки: логіни, об’єкти, політики, створення процесів тощо.
    - System — події ядра й системних компонентів: драйвери, живлення, збої.
- Applications and Services Logs — докладні журнали конкретних компонентів, наприклад Microsoft-Windows-PowerShell/Operational, Microsoft-Windows-Sysmon/Operational (якщо встановлено Sysmon (System Monitor)), RemoteDesktopServices тощо.
- Forwarded Events — журнал, куди надходять події з інших хостів (при налаштованому зборі).

3. Типові сценарії використання у DFIR (Digital Forensics and Incident Response)

- Розслідування компрометації облікових записів: 4624/4625/4672, типи логонів, джерельні IP (Internet Protocol address), SID (Security Identifier).
- Встановлення і запуск шкідливого ПЗ: 4688 «створено процес», кореляція з командними рядками, батьківськими процесами, шляхами виконуваних файлів.
- Persistence і зміни політик: 4719 зміна політики аудиту, 4670 зміни дозволів.
- Ескалація привілеїв: 4672 «special privileges assigned».
- Приховування слідів: 1102 очищення журналу аудиту.

4. Підходи до аналізу

- Pivot від «віх» подій: наприклад, фіксуємо незвичний логон і шукаємо навколо нього процеси, мережеві події, зміни політик у близьких мітках часу.
- Кореляція через поля EventData: TargetUserName, LogonType, ProcessName, CommandLine, ParentProcessName, IpAddress, WorkstationName.
- Експорт у EVTX/CSV (Comma-Separated Values) і подальший аналіз у інструментах: Event Viewer, PowerShell, wevtutil, ELK (Elasticsearch, Logstash, Kibana)/Splunk, Chainsaw, Timeline-побудова.

Практична частина

Виконайте кроки на своїй VM із Windows 10/11. За потреби згенеруйте активність: логін/лог-аут, запуск процесів, зміна політик, вимкнення/увімкнення тощо.

Крок 1. Перегляд журналів у Event Viewer

1. Відкрийте Event Viewer: Win+R → eventvwr.msc.
2. Перейдіть до Windows Logs та по черзі перегляньте Application, Security, System.
3. У правій панелі використайте «Filter Current Log...» для обмеження за часом, рівнем, Event ID або ключовими словами.

Крок 2. Базові фільтри для Security

- Перевірте логіни та привілеї:
  - 4624 Успішний вхід. Важливо: LogonType, IpAddress, TargetUserName.
  - 4625 Невдалий вхід. Зіставте з джерелом та обліковим записом.
  - 4672 Призначено спеціальні привілеї новому сеансу.
- Створення процесів:
  - 4688 Створено новий процес. Перегляньте поля NewProcessName, CommandLine, ParentProcessName.
- Зміни політик/конфігурацій:
  - 4719 Змінено політику аудиту системи.
  - 4670 Змінено дозволи доступу до об’єкта.
- Очищення та цілісність журналів:
  - 1102 Журнал аудиту очищено.

Крок 3. Перегляд System та Application

- System: зверніть увагу на 41/6008 (некоректне вимкнення), події драйверів, служби живлення.
- Application: помилки застосунків, збої служб, події групових політик (на кшталт 1125).

Крок 4. Операційні журнали компонентів

- Розгорніть Applications and Services Logs → Microsoft → Windows і перегляньте, наприклад:
  - PowerShell → Operational: пошукайте запуск скриптів та збережені командні рядки.
  - RemoteDesktopServices, TerminalServices: логіни по RDP (Remote Desktop Protocol).
  - Якщо у вас встановлено Sysmon — Microsoft-Windows-Sysmon/Operational для детальних процесів, мережі, модулів.

Крок 5. Експорт і командні інструменти

- Експорт обраного журналу у .evtx або .csv через Save All Events As...
- PowerShell приклади:
  - Отримати останні 50 подій 4688: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4688} -MaxEvents 50 | Format-List`
  - Фільтр за часом: `Get-WinEvent -FilterHashtable @{LogName='Security'; StartTime=(Get-Date).AddHours(-2)} | where Id -in 4624,4625,4672,4688 | Select TimeCreated, Id, ProviderName, Message`

Крок 6. Міні-розслідування

- Створіть таймлайн із подій за останні 2–4 години навколо вашої штучно згенерованої активності.
- Відповісти: хто/коли увійшов, які процеси запускалися, чи були зміни політик, чи є ознаки очищення журналів.

Довідкові Event ID (корисні для пошуку)

Код події	Короткий опис	Журнал	Тип події	Критичність
4624	Успішний вхід	Security	Success	Середня
4625	Невдалий вхід	Security	Failure	Середня
4634	Завершення сеансу (logoff)	Security	Information	Низька
4648	Вхід із явним зазначенням	Security	Information	Середня

Код події	Короткий опис	Журнал	Тип події	Критичність
	облікових даних			
4672	Призначено спеціальні привілеї новому сеансу	Security	Success	Висока
4673/4674	Використання чутливих привілеїв / Спроба використання привілею	Security	Success/Failure	Висока
4688	Створено новий процес	Security	Information	Висока
4697	Встановлено нову службу	Security	Success	Висока
4719	Змінено політику аудиту системи	Security	Success/Failure	Висока
4720	Створено обліковий запис користувача	Security	Success	Висока
4726	Видалено обліковий запис користувача	Security	Success	Висока
4732	Користувача додано до локальної групи	Security	Success	Середня
4776	Перевірка облікових даних у контролера домену (NTLM)	Security	Success/Failure	Середня
5156	WFP дозволив мережеве	Security	Information	Середня

Код події	Короткий опис	Журнал	Тип події	Критичність
	з’єднання			
7045	Сервіс інстальовано у системі	System	Information	Висока
1102	Журнал аудиту очищено	Security	System	Висока
41/6008	Система критично закінчила роботу	System	Error/Critical	Висока
1125	Помилка застосування групової політики	Application	Error	Середня